CorreLog®

SQL Table Monitor Adapter

Users Manual

http://www.correlog.com mailto:info@correlog.com

CorreLog, SQL Table Monitor Users Manual

Copyright © 2008 - 2015, CorreLog, Inc. All rights reserved.

No part of this manual shall be reproduced without written permission from the publisher. No patent liability is assumed with respect to the use of the information contained herein. Although every precaution has been taken in the preparation of this book, the publisher and author assume no responsibilities for errors or omissions. Nor is any liability assumed for damages resulting from the use of this information contained herein.

Table of Contents

Section 1: Introduction	……..	5
Section 2: Software Installation	……..	9
Section 3: Software Operation	……..	13
Alphabetical Index	……..	29

Section 1: Introduction

This manual provides a detailed description of the CorreLog SQL Table Monitor software. This is an optional set of files and executables added to the CorreLog Server order to expand the role of the CorreLog to include event monitoring of changes or additions to one or more Relational Database tables.

The adapter executes user defined SQL queries, reads and processes the results of these queries, and converts these results into Syslog messages that are used by CorreLog Server.

The manual provides information on specific features and capabilities of this special software, including installation procedures, operating theory, application notes, and certain features not documented elsewhere.

The SQL Table Monitor software consists of several components. A background process continuously executes a series of SQL statements at periodic intervals. The results of these SQL statements are compared to match patterns. Messages are sent to the CorreLog server when patterns are matched. Additionally, the user can inspect specific SQL responses.

This manual is intended for CorreLog users who will operate the system, as well as system administrators responsible for installing the software components. This information will also be of interest to program developers and administrators who want to extend the range of the CorreLog to include monitoring of log messages stored in SQL Tables.

Overview Of Operation

The SQL Table Monitor Adapter software extends the CorreLog system to permit periodic checking of data within a relational database. This allows CorreLog to actively monitor event data residing in a database.

The CorreLog SQL background process periodically executes SQL statements on ODBC data sources, compares SQL responses to threshold values (in the form of match patterns), and then sends Syslog messages (of user specified severity and content) to the main CorreLog server when patterns are matched. This gives CorreLog more awareness of the network and enterprise state by monitoring the data that may reside in ODBC compliant databases.

The CorreLog SQL background process is configured and monitored using a tightly coupled integration with the main CorreLog web interface. The user configures simple or complex SQL statements, and defines the message and severity that is sent to CorreLog when responses are matched.

SQL Table Monitor System Software Components

The CorreLog SQL Table Monitor comes as a single downloadable package in self-extracting WinZip format. This package is installed at the CorreLog server, and contains the following specific components.

- **CO-sqlmon.exe Program.** This is the polling agent that is responsible for gathering SQL information on the system. The process is configured to run on CorreLog system startup (via the "System > Schedule" screen, as documented below.)

- **SQL Table Monitor Configuration Screen.** This is a support screen, available under the "Messages > Adapters > SQLMon" tab of the CorreLog web interface as part of the Windows component installation. This screen allows the user to configure the SQL queries to be performed, as well as configure match patterns and messages that are sent when events are detected.

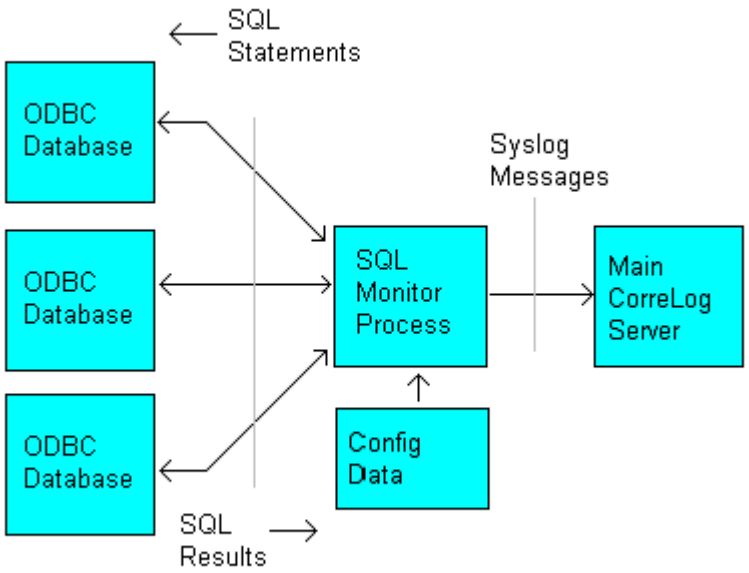
These two items cooperate to allow full monitoring of events that are stored in SQL databases, including different databases residing on remote platforms. The CO-SQLMon.exe program runs as a persistent background process, and the SQL Table Monitor Configuration Screen allows the operator to configure this process and the queries it executes.

System Block Diagram

The CorreLog SQL Table Monitor process consists of a single background process, which executes at the CorreLog server. This process reads configuration data that has been configured by the operator, and continuously executes a list of SQL statements at a particular poll rate (by default each 30 seconds.) These SQL statements are applied against ODBC compatible databases. The databases can be local to the CorreLog server, or reside on other platforms on the network.

When each SQL statement is executed, the results of the statement are fetched and compared to match patterns, and to previously queried results. Each row of the results is treated as a single event record (i.e. a single line) and compared to match patterns configured by the operator. If the match pattern is satisfied, the matched record is sent to CorreLog as an event message with a severity specified by the operator.

Once the Main CorreLog Server has received the message, it is treated like any other syslog message, and can be further correlated using Threads, Alerts, Triggers, and tickets.



As indicated in the above diagram, the SQL Table Monitor Process (i.e. the CO-SQLMon.exe process, which is installed and configured as described in the next chapters) continuously sends SQL statements to one or more ODBC databases. These can be local databases, or remote databases. They can be a single database in the enterprise, or many different databases including Access, Oracle, MS-SQL, and other database items.

The polling process is completely controlled and monitored by data that is configured by the operator using the "Messages > Adapters > SQLMon" screen of the Main CorreLog Server web interface.

SQL Table Monitor Constraints

The SQL Table Monitor is designed to permit a large amount of flexibility. However, there are several constraints to its operation that must be considered:

1. The SQL Table Monitor requires an ODBC interface.

2. The SQL Table Monitor is limited to a maximum number of results per polling cycle (by default 100 records per 30 seconds). Any data returned from a database query above this value will be lost. Note that this limit applies ONLY to the results, and not necessarily the number of records actually scanned or queried. This value is adjustable to a maximum of 1000 results for each SQL query.

3. The SQL Table Monitor tracks data ONLY while the CorreLog server is running, and has no provision for obtaining records that are logged if the CorreLog server is rebooted, or temporarily shut down.

How To Use This Manual

The next section of this manual (Section 2) provides the essential information needed to install the CorreLog SQL Table Monitor Adapter software. Note that the only required components of the system are the CO-SQLMon.exe program and the SQL configuration screen, documented herein. Other information on the CorreLog server can be found in the standard "User Manual", including operation and application notes that will be of assistance in processing the SQL messages generated by the CO-SQLMon.exe program, and received by the CorreLog Syslog receiver process.

Section 2: Software Installation

The CorreLog SQL Table Monitor software is usually delivered as a self-extracting WinZip file. The installation requires a few simple manual installation steps, and no automatic installation is provided or required. The basic installation steps are as follows:

1. The user obtains the CorreLog SQL Table Monitor software, in self-extracting WinZip format.

2. The user stops the CorreLog Server background processes.

3. The user executes the self-extracting WinZip file (obtained in step 1 above). This unzips the SQL software into the CorreLog Windows Distribution, including all configuration data and executables.

4. The user restarts the CorreLog Server background processes.

5. The user configures queries and other items via the newly added "Messages > Adapters > SQLMon" screen.

6. The user configures other parts of the CorreLog system, such as Threads, Alerts, and Ticket users, to correlate and process the syslog messages that are generated by the SQL Table Monitor software.

Administrative logins are required in order to perform the software installation. The detailed steps needed to perform the installation are provided in the sections that follow.

Installation Requirements

The SQL Table Monitor software is minimally invasive, and can be installed on a variety of platforms and operating systems.

- **Existing CorreLog Server Installation.** Prior to installing the SQL Table Monitor software, the CorreLog Server system must be installed on a Windows platform, as discussed in the CorreLog User Reference Manual.

- **Disk Space Requirements.** The SQL Table Monitor software requires no significant disk space beyond the normal footprint of the CorreLog server. There is generally no extra disk space load due to this software.

- **CPU Requirements**. The SQL Table Monitor software requires very little extra CPU requirements. A single process is started the CorreLog Windows platform, which consumes minimal CPU resources.

- **Firewall Requirements.** The SQL Table Monitor software requires that managed devices respond to Relational Database SQL requests from the CorreLog server. This is the normal condition (however some sites may purposely disable SQL ODBC queries from devices, and those selected devices will not be manageable by CorreLog.)

- **Database Requirements.** The SQL Table Monitor requires an ODBC connection to a database that has been configured via the Windows Control Panel > Admin Tools facility. The ODBC data source must also be configured via the CorreLog "Reports > ODBC". Additional constraints, (discussed in Section 1) also exist.

To insure proper installation of the program, the user should close all windows, and temporarily disable any port blocking or Virus Scan software on the system. The existing CorreLog server process should be stopped prior to the installation. Reboot, after installation, is not required.

Windows Installation Procedure

The specific steps needed to install the software are as follows:

1. Login to the CorreLog Server Windows platform using an "Administrator" type login.

2. Stop the CorreLog Server processes via the Windows Service Manager, or via the "Start and Stop Services" utility found in the Windows Start

menu, or via a "net stop correlog" command prompt statement. Verify with the Windows "Task Manager" that all CorreLog processes are stopped.

3. Obtain and execute the "co-n-n-n-sqlm.exe" package, extracting files to the directory location where CorreLog is installed (by default the location "C:\CorreLog"). This installs the appropriate files and modifies CorreLog to start the "CO-SQLmon.exe" program when the CorreLog system starts.

4. Restart the CorreLog Server processes via the Windows Service manager, or via the "Start and Stop Services" utility, or via a "net start correlog" command prompt statement.

5. Verify with the Windows "Task Manager" that the "CO-SQLMon.exe" process is now running on the system, along with the other CorreLog processes.

SQL Software Configuration

Once the CO-SQLMon.exe program has been installed and is running on the system, the user can configure the ODBC data sources and queries to be executed. The user must first define the ODBC data sources, and then define the SQL statements, match patterns, and syslog message severities.

Basic steps to the configuration are as follows:

1. First, the user creates an ODBC data source via the "Control Panel > Admin Tools" of the Windows system. This provides a data source name (used in the second and third parts of the procedure. The operator must configure a "System" type DSN.

2. Once the System DSN / ODBC data source has been created, the operator logs into CorreLog and accesses the "Reports > ODBC" screen. (The name selected in Step 1 above will appear in the drop down list of data sources.) The operator configures the ODBC data source, including any required username and password.

3. Once the ODBC data source has been configured on the "Reports > ODBC" screen of CorreLog, the operator can create an SQL Table Monitor via the "Messages > Adapters > SQLMon" tab of the system. Specific steps explaining how to do this are provided in the next section of this manual.

The above steps may be sufficient to start using the SQL Table Monitor immediately. More information on the configuration steps needed to monitor the SQL database is provided in the next section, including application notes and caveats.

Section 3: Software Operation

The CorreLog SQL Table Monitor software allows the user to incorporate database information, particular database events, into the correlated stream of messages.

Three separate modes of operation are available to the operator: "Update Monitoring", "Change Monitoring", and "Tail Monitoring" of database tables. Each of these three operating modes, including their configuration and their application, are described in this section.

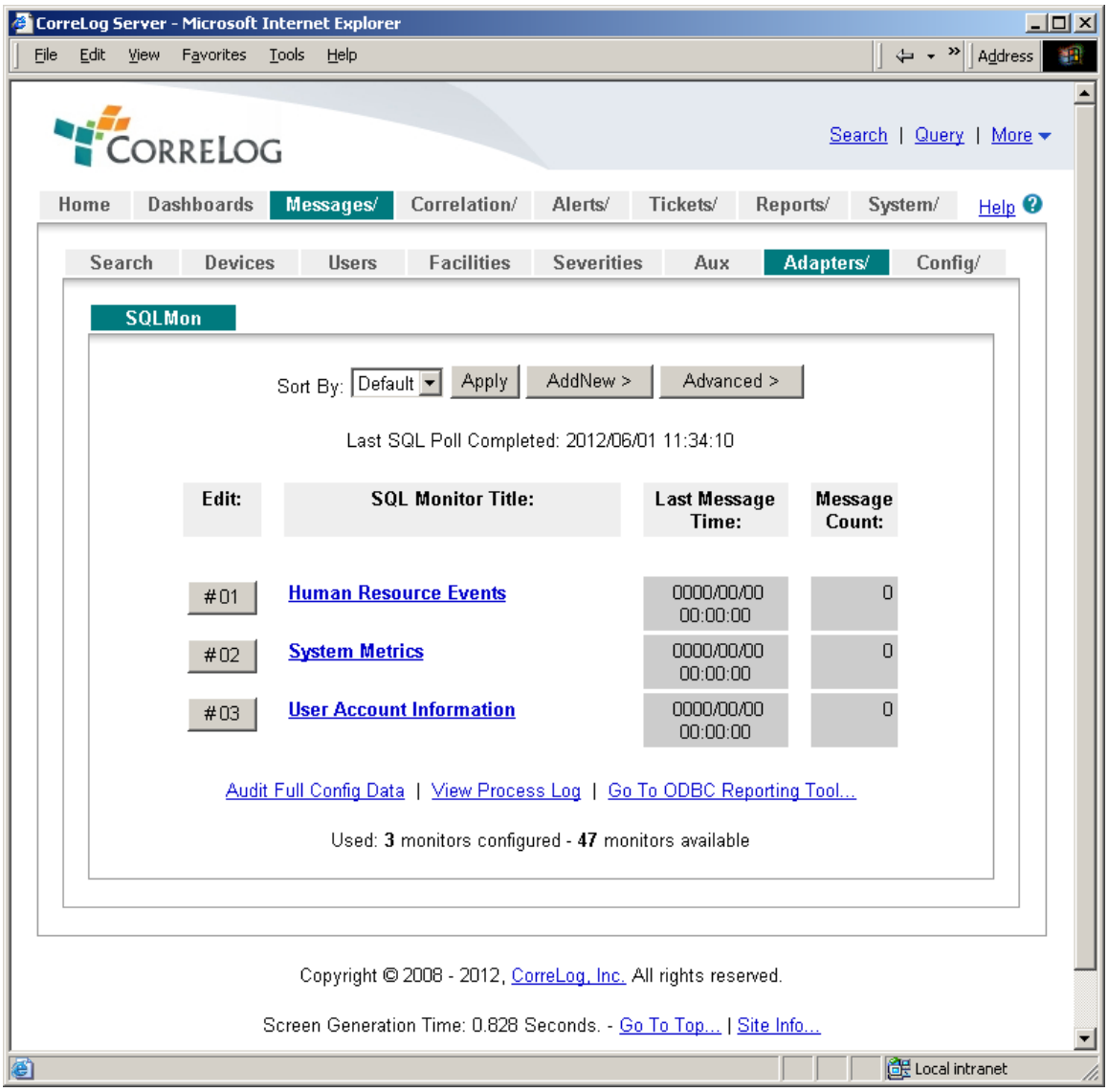
Because of the flexibility of SQL, this provides an excellent avenue for system developers and integrators to add special functionality and capability to CorreLog in a manner that might otherwise be difficult or impossible to implement. The SQL record data is mixed with the Syslog messages and / or SNMP traps, giving new visibility into the current state of the managed enterprise.

The CorreLog SQL Table Monitor program requires very limited operating notes. Once the program is installed, it makes use of reasonable default values. The operator only needs to specify the queries and data sources to be polled.

This section provides a description of these optional software elements, their usage, and other considerations, including screenshots and explanation of monitor configuration values.

SQL Table Monitor Screen

As part of the Windows installation, a new tab is created in the "Message > Adapters" section of the CorreLog web interface, which permits the user to configure various parameters associated with the SQL Table Monitor program. To add a new monitor to the system, the user clicks the "AddNew" button. A typical top-level screen is shown below,


CorreLog Server - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address
CORRELOG
Search | Query | More
Home Dashboards Messages/ Correlation/ Alerts/ Tickets/ Reports/ System/ Help
Search Devices Users Facilities Severities Aux Adapters/ Config/
SQLMon
Sort By: Default Apply AddNew > Advanced >
Last SQL Poll Completed: 2012/06/01 11:34:10
Edit: SQL Monitor Title: Last Message Time: Message Count:
#01 Human Resource Events 0000/00/00 00:00:00 0
#02 System Metrics 0000/00/00 00:00:00 0
#03 User Account Information 0000/00/00 00:00:00 0
Audit Full Config Data | View Process Log | Go To ODBC Reporting Tool...
Used: 3 monitors configured - 47 monitors available
Copyright © 2008 - 2012, CorreLog, Inc. All rights reserved.
Screen Generation Time: 0.828 Seconds. - Go To Top... | Site Info...
Local intranet

The above screen shows typical values: Three different SQL monitors are defined that periodically query data. The user can add a new monitor via the "AddNew" button, or can edit (or delete) an existing monitor via the "Edit #NN" button for the monitor. The user can click down into a hyperlink for more detailed information, and can configure advanced options via the "Advanced" button.

SQL Monitor Types

When creating a new SQL Monitor item via the "AddNew" button, the operator first selects a type and mode for the monitor. Three types of SQL Monitors are supported, and each monitor operates is a slightly different manner, described below:

- **Update Monitor.** This type of monitor is mainly useful when operating on a table where specific elements are updated, or sometimes added. The query executes and selects a small number of records (typically under 100, but potentially as many as 1000 records. Each record is compared with the results of the previous query (automatically retained by the system) and any new records are converted to syslog messages. For example, the user may query a table to determine when certain values are "less than", "equal to", or "greater than" some value. Any new records resulting from the query are converted into syslog messages.

- **Change Monitor.** This type of monitor is similar to an "Update" monitor (described above) except that the system reports when new records exist in a query's results, or are absent from the previous results of the query. The query executes and selects a small number of records, as with the "Update Monitor". Each record is compared with the results of the previous query (automatically retained by the system). If a new record exists, or a record in the previous query results does not exist, then these records are converted into syslog messages. This provides a method of determining whether records have been added, deleted, or modified since the last time the database table was polled.

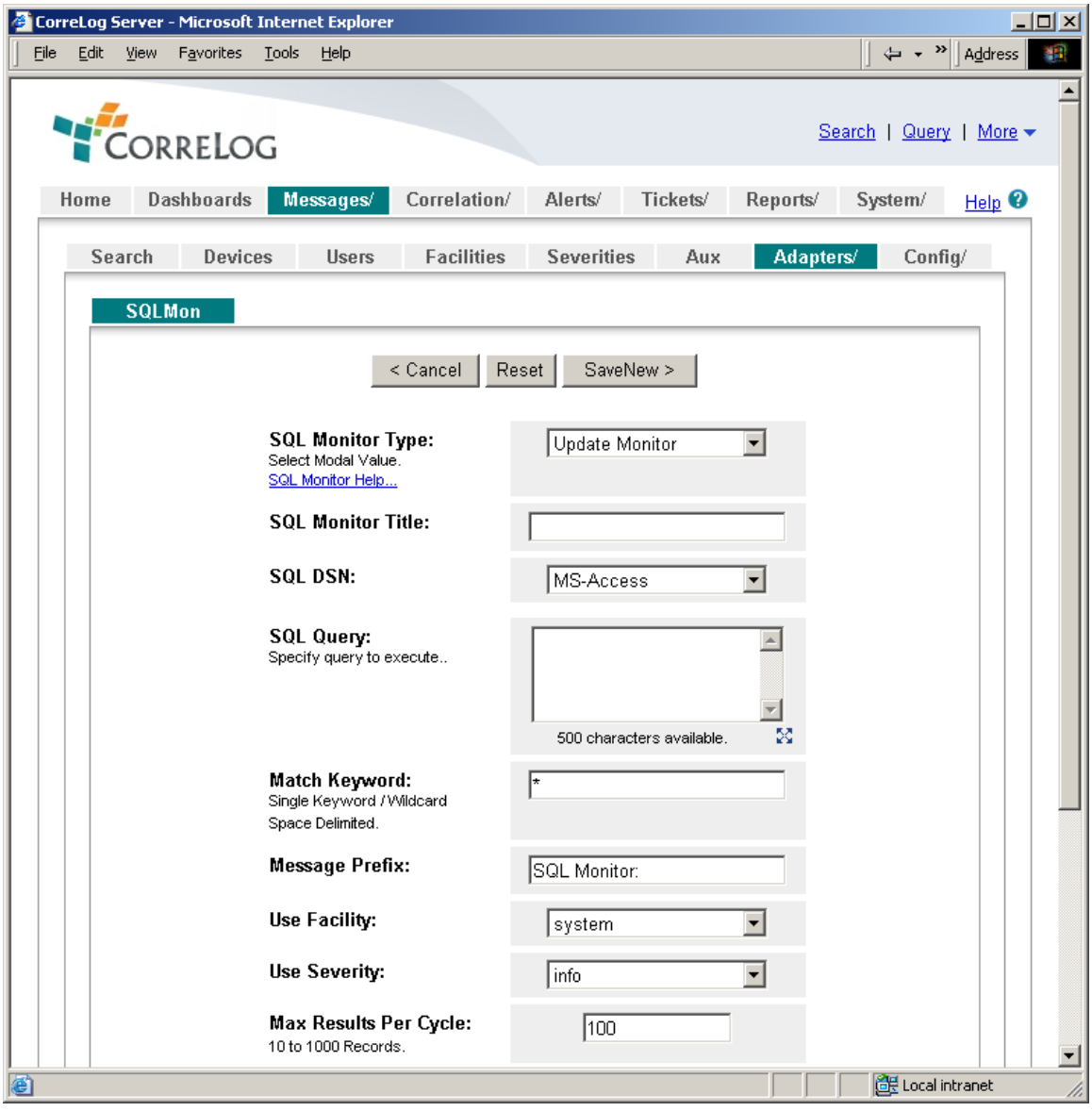
- **Tail Monitor.** This type of monitor is distinctly different than either the "Update" or "Change" monitor types described above. This type of monitor performs the highly specialized (but fairly common) case of a streaming log file contained in a database table. The specified table must have a numerically or lexically increasing index value. Each time the query executes, it selects records that have a higher index than the previous query, resulting in any new records that have been added to the system to be converted to syslog messages. The function described here is similar to "tailing a log file" (such as with the CorreLog "Log File Monitor" function), but the operation occurs on a database table.

- **Tail Monitor (Adv).** This type of monitor performs a function identical to the "Tail Monitor" above, except that it permits the user to configure a more advanced query, possibly consisting of table joins. The first column of the query result is taken as the index value. Otherwise, the operation is identical to the "Tail Monitor" described above.

The default monitor type is an "Update Monitor", which is mainly useful when a group of records is being periodically updated. The "Tail" monitor is more specialized, and can be used to access records in a large database, where certain records are continuously appended to a table and indexed by an increasing value (such as an incrementing record number, or a timestamp.)

Update and Change Monitor Configuration

The "Update" and "Change" monitor type of configuration both query a small set of values (typically under 100 but potentially up to 1000 records.) Both of monitor types have the same input fields. (Selecting the SQL Monitor Type of either "Update Monitor" or "Change Monitor" displays the appropriate fields. The "AddNew Update Monitor" screen is depicted below.



The above screen is a standard CorreLog dialog, and is the default screen when the user clicks the "AddNew" button. If the user selects the "SQL Monitor Type" to be either "Update Monitor" or "Change Monitor", the fields for the screen are described below.

- **SQL Monitor Title.** This is a short title that appears on the top-level SQL Table Monitor page, used to quickly identify the nature and purpose of the monitor function, usually the same as the type of query being executed.

- **SQL DSN.** This is a configured ODBC Data Source Name (DSN). The DSN is configured first in Windows (via the "Administrative Tools" screen) and then is configured in the "Reports > ODBC" screen (to assign login parameters.) When the user configures the CorreLog Reports > ODBC screen, the DSN will appear in this drop-down menu and can be selected by the user.

- **SQL Query.** This is the query that is executed by the system, and should be designed to return a small number of records that are being monitored. The number of records returned should be less than the "Max Results Per Cycle" value, described below.

- **Match Keyword.** This is a keyword or wildcard that is applied against each row of the results. When any result matches the keyword, the result is converted into a syslog message and sent to CorreLog.

- **Message Prefix.** This is an additional keyword and message prefix, such as the table name, or any other arbitrary text that can be used to correlate the data or identify the data source. The value is applied to each message generated by the monitor.

- **Max Results Per Cycle**. This is an optional value that can limit the number of messages that are sent to CorreLog for each query. (This value prevents millions of messages from being sent to CorreLog based upon the results of a particular query.) If this value is exceeded, the SQL monitor sends a special error message to CorreLog, described in a later section. See additional notes below.

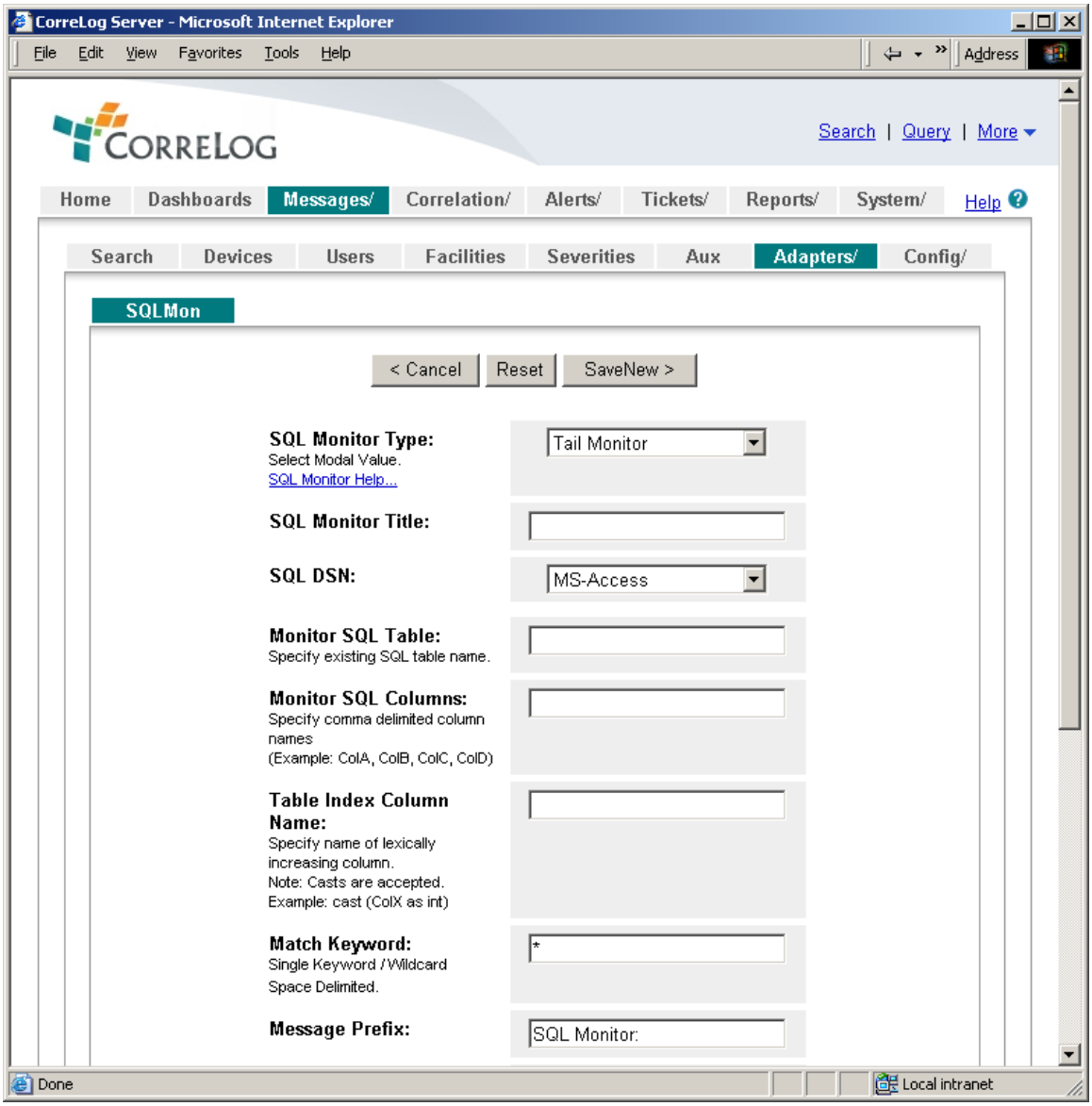
- **Use Facility.** This is the syslog facility for the message that is generated by the CO-SQLMon.exe program when the specified pattern is matched. It can be selected to be any standard facility code.

- **Use Severity.** This is the severity of the message that is generated by the CO-SQLMon.exe program when the specified pattern is matched. It can be selected to be any standard severity code.

The operation of the "Update Monitor" and "Change Monitor" types are similar, but have important differences. The "Update" monitor is much more efficient, and reports only when records are changed or have been added to the result set. In contrast, the "Change" monitor requires slightly more CPU, and will report whether records have been added or deleted from the results set.

Tail Monitor Mode

The "Tail" monitor type of configuration operates in a different manner than the "Update" or "Change" monitor types. This type of monitor can be used to tail a large table that is continuously appended with new records. The specified table must have an "Index" column containing a unique and incrementing value. Selecting the "Tail Monitor" type displays the appropriate configuration fields. The "AddNew Tail Monitor" screen is depicted below.



The above screen is a standard CorreLog dialog, and is displayed when the user clicks the "AddNew" button, and then selects the "SQL Monitor Type" to be "Tail Monitor". The fields for the screen are described below.

- **SQL Monitor Title.** This is a short title that appears on the top-level SQL Table Monitor page, used to quickly identify the nature and purpose of the monitor function, usually the same as the type of device or network segment being polled.

- **SQL DSN.** This is a configured ODBC Data Source Name (DSN). The DSN is configured first in Windows (via the "Administrative Tools" screen) and then is configured in the "Reports > ODBC" screen (to assign login parameters.) When the user configures the CorreLog Reports > ODBC screen, the DSN will appear in this drop-down menu and can be selected by the user.

- **SQL Monitor Table.** This is the name of an existing table that will be monitored. The table must exist, and it must have at least one column that is either alphabetically or numerically increasing in value that will be used as the "Table Index Column Name" described below.

- **Monitor SQL Columns.** This is a list of the column names that will be queried by the program to compose the resulting message (with one message per row.) The columns must be separated by commas, and can be any textual or numeric value. The list can include the "Table Index Column" name (below) but that column name is automatically included and does not need to be specified here.

- **Table Index Column Name.** This is the name of the index column that will be used to sort and order the data. The column must have a unique and increasing value, and may be named such as "MSGNO", "TSTAMP", or "LOGTIME". The actual column name will be checked by the program prior to saving the data. (See "Constraints" in "Section 1" of this manual.) This value can include a "Cast" statement, such as to cast a timestamp into an integer value. (See additional notes below.)

- **Match Keyword.** This is a keyword or wildcard that is applied against each row of the results. When any result matches the keyword, the result is converted into a syslog message and sent to CorreLog.

- **Message Prefix.** This is an additional keyword and message prefix, such as the table name, or any other arbitrary text that can be used to correlate the data or identify the data source.

- **Max Results Per Cycle**. This is an optional value that can limit the number of messages that are sent to CorreLog for each query. (This value prevents millions of messages from being sent to CorreLog based upon the results of a particular query.) See additional notes below.

- **Use Message Facility.** This is the syslog facility for the message that is generated by the CO-SQLMon.exe program when the specified pattern is matched. It can be selected to be any standard facility code.

- **Use Message Severity.** This is the severity of the message that is generated by the CO-SQLMon.exe program when the specified pattern is matched. It can be selected to be any standard severity code.

Tail Monitor, Table Index Column Additional Notes

When using a "Tail Monitor", each table requires at least one column that is numerical or textual, and increasing in value. CorreLog will transmit messages after successfully retrieving the last value. If the index column is not numerically increasing this can cause the SQL Table Monitor to skip records, or actually hang. These situations can be investigated and debugged using the "Reports > ODBC" tab to query and inspect the table.

It may be necessary to "cast" a value to a numeric value. For example, depending upon the database and table, the user may have a type "timestamp" column, and this column may be configured to output a date and time that is not convenient for processing.

For example, on MS-SQL, the user may have a table column named "IXCOL", which contains values of type "timestamp". (The "timestamp" values contain entries that are automatically updated with the system time whenever a row is inserted.) In this case, the operator can specify the timestamp value as follows:

```
Cast (IXCOL as int)
```

Most (but not all databases) will permit the above syntax to be applied directly as the "Table Index Column" name, which forces the query to treat the "IXCOL" column name as an integer value, appropriate for indexing the rest of the table.

Tail Monitor (Adv) Setting

The above tail monitor configuration is useful for relatively simple queries, except that it suffers from the inability to create more complex queries. To permit a regular query, the operator can select the "Tail Monitor (Adv)" setting (where "Adv" indicates "Advanced", for more advanced users.) This type of query should generally be avoided unless absolutely necessary, since the error checking of the query is somewhat limited, and debugging the query can be complicated. For assistance, please contact CorreLog support.

Max Results Setting

Each database query configured by the operator has its own "Max Results" value, which is the maximum number of results returned by a query.

Note that this value is not necessarily the number of records processed by the query (which can be enormous), but the number of results returned by the query. If any query returns more than the maximum number of results, an error is generated (as described below) and the remaining results are discarded.

This setting implies that the operator must return a limited result, such as the number of records where a value is greater than, equal to, or less than some other value. For example, acceptable queries by the "Update" and "Change" monitor modes include the following:

```
Select * from MyTable Where IntValue < 100

Select * from MyTable Where TextVal like '%Test%'

Select Distinct UserID, UserGroup from MyTable

Select Count (*) from MyTable
```

The above queries each return some result set that is less than the entire contents of the database, hence are likely acceptable queries. Any of the above queries that return a value of more than "Max Results" requires the user to either adjust the query, or set the value of "Max Results" to a higher value.

Each record returned by a query is potentially a message that is sent to the operator. Therefore, if the "Max Results" setting is 100, there can only be a maximum of 100 messages sent to CorreLog for any given SQL monitor. The "Max Results" value limits the amount of data that must be converted to syslog messages. Without a "Max Results" setting, a query could potentially return millions (or hundreds of millions) of records, each of which may be a syslog message correlated and stored by the CorreLog Server.

Generally, the default "Max Results" value of 100 records should be satisfactory for most applications, implying that the most syslog messages sent by any particular SQL query is 100 messages or less.

Error Handling And Debug

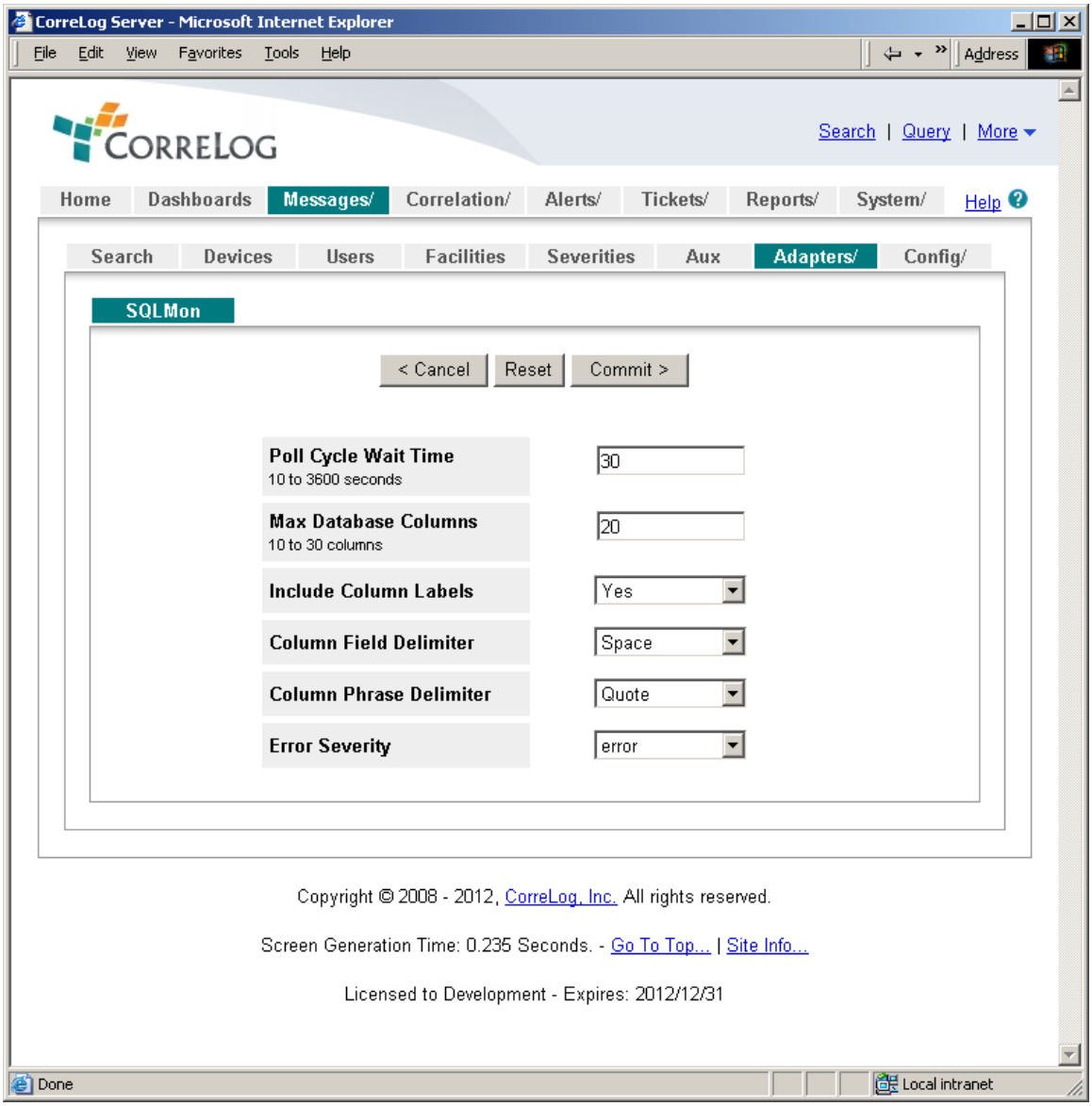
The user table specification, including the table name, table column index, and other column names, are checked for appropriateness before any data is saved. While saving the data, if any value is misconfigured, an error will be displayed and the data is not saved.

The error displayed when saving the data is returned directly from the database. Therefore, error messages depend upon the type of database being monitored. The operator may have to consult the specific documentation for the database to fix certain errors. The operator can execute the "Reports > ODBC" screen to run queries on the target table to investigate and resolve the error.

As a special case, if any configured query returns more than the "Max Results" value, then a special error message is sent to the CorreLog server indicating the name of the SQL Monitor that should be adjusted. This error may be generated each time a query returns more than the expected maximum number of results.

Advanced Settings Screen

The user can click the "Advanced" button on the top-level screen to display several advanced settings of the SQL Table Monitor. These settings generally require no adjustment, but can be used to further tune the monitor system. The specific settings permit the user to adjust the poll rate of the system (by default each 30 seconds), and specify the maximum number of database columns. The "Advanced Parameters" screen is depicted below:



The above screen is a standard CorreLog dialog. The user modifies the screen values and clicks "Commit" to save them. The fields for the screen are described below:

- **Poll Cycle Wait Time.** This value determines the time between executing a query cycle. The default value is 30 seconds, which means that queries are executed on the ODBC data sources twice each minute. The value can be increased to some higher value (such as 1 hour) to reduce the loading on the database, but longer polling intervals will reduce the real-time aspect of the system.

- **Max Database Columns.** This value determined the maximum number of database columns that are returned by a query. If more than this number of columns are returned by a query, the extra columns are eliminated from the query. This reduces the width of the message, which may be desireable in order to reduce the syslog loading of the adapter. The default value is 20 columns.

- **Include Column Labels.** This value affects the format of the syslog messages generated by the adapter. The default value of "Yes" causes the column name of the database table to prefix each column value, for easier interpretation of the message and the expense of message size.

- **Column Field Delimiter.** This value affects the format of the syslog messages generated by the adapter. The default value of "space" indicates that each column value is delimited by a space. The user can change the value to some other punctuation mark to assist in parsing the message.

- **Column Phrase Delimiter.** This value affects the format of the syslog messages generated by the adapter. The default value of "quote" indicates that the data of each column is contained in double quote marks, which permits easy parsing by the "Pivot" report or other CorreLog reporting features.

- **Error Severity.** This value is the severity of any self-detected errors, such as a query that fails, or some overflow condition. The default value is "error", indicating any errors are send with this severity to the CorreLog server. The special value of "disabled" will disable any self-error reporting.

Note that adjusting any parameter here will automatically reinitialize the entire SQL polling cycle, discarding any current data that may exist and restarting the system as if the CorreLog Server was restarted.

Creating Threads, Tickets, and Alerts

Because the messages sent by the SQL Table Monitor are the control of the operator, it is easy to create threads, tickets and alerts that will correlate and reduce the monitor's message into actionable data. The basic method for

correlating the SQL Table Monitor messages is no different that the techniques discussed elsewhere. The basic steps are provided below.

1. The operator creates a thread to tabulate the messages sent by the monitor using the "Correlation > Threads > Add New" screen. This screen is used to collect all the messages of a particular type (such as all messages with "Router" in the match results, possibly further qualified by a particular address group, severity, or time of day.)

2. The operator creates an Alert for the thread counter using the "Alerts > Counters > Add New" screen. This alert will send a Syslog message back to the main list of messages when one or more messages are received during an interval of time. As is always the case, when an alert is triggered, a single message is sent back to CorreLog, and a single ticket is opened while the alert is set. (See additional notes below.)

3. The operator optionally identifies an "Assignee" for the alert via the "Alerts > Counters > Add New" screen. This causes a ticket to be opened on the system, and assigned to a particular user or a ticket group. The user can assign a ticket to any existing user, or ticket group.

4. The operator optionally adds a "Ticket Action" to the system, which sends e-mail (or performs some other action) when a new ticket is opened on the system, providing a real-time indication that a timeout threshold of the SQL Table Monitor software has been violated. This message will typically contain the descriptive text entered by the operator when the alert was created, which may be slightly (or totally) different than the originating SQL Table Monitor message.

As a special note, if only one ticket is to be opened on the system per SQL threshold violation (as will often be the case), then the "Alert Interval", configured on the "Alerts > Counter" screen, should be higher than the "Poll Interval" displayed at the lower left of the "Messages > Adapters > SQL" screen. Additionally, the "Auto-Learn" function for the alert should probably be disabled to prevent this interval from changing automatically.

Failure to understand or implement this consideration may result in multiple tickets being opened for the same system threshold violation, which will not be desirable, especially if one of the ticket actions is to send e-mail or provide other intrusive notifications to the ticket assignee.

Section Summary, Additional Notes

1. The CO-SQLMon.exe program polls a database using a query composed on the "AddNew" screen. For any query results that match the specified

pattern, a syslog message is issued to CorreLog containing the matched row.

2. Three different types of monitoring can occur, selected when the user creates the SQL Monitor entry. The user can specify a monitor type of "Update", "Change", or "Tail".

3. The "Update" and "Change" monitor types are used to determine whether a change has occurred in a database result set. The expected result set should be small (typically 100 lines or less) and should be less than the "Max Results" setting of the monitor.

4. The "Tail" monitor type is used to tail records of a possibly large table, and reports any new records that are added to the table. This monitor type requires an index to the table that contains an increasing value such as a timestamp or record number.

5. The "Advanced" screen can be used to adjust certain parameters such as the "Poll Cycle Wait" time, which affects the rate at which configured queries are executed on the system, and affects the loading of the database.

6. Change to the "Advanced" screen will restart all monitoring, discarding any pending data that may exist, and reset the message times, error counts, and other items of each SQL monitor. The process resumes exactly as if it was restarted.

7. The user can determine the poll time and response time for the CO-SQLMon.exe program by drilling down into the SQL Table Monitor name hyperlink, which shows the current response time values for all devices during the last poll cycle.

8. When configuring a CorreLog alert, the "Alert Interval" should be greater than the "Poll Interval" value to prevent multiple tickets from being opened for a single incident. Additionally the "Auto-Learn" function for the alert should typically be disabled.

For Additional Help and Information…

Detailed specifications regarding the CorreLog Server, add-on components, and resources are available from our corporate website. Test software may be downloaded for immediate evaluation. Additionally, CorreLog is pleased to support proof-of-concepts, and provide technology proposals and demonstrations on request.

CorreLog, Inc., a privately held corporation, has produced software and framework components used successfully by hundreds of government and private operations worldwide. We deliver security information and event management (SIEM) software, combined with deep correlation functions, and advanced security solutions. CorreLog markets its solutions directly and through partners.

We are committed to advancing and redefining the state-of-art of system management, using open and standards-based protocols and methods. Visit our website today for more information.

CorreLog, Inc.
http://www.CorreLog.com
mailto:support@CorreLog.com

Alphabetical Index

A

Access / 7
Action / 23
Adapter / 6 8 27
Adapters / 6 8 9 11 14 23
Addnew / 14 15 16 18 23
Admin / 10 11
Administrative / 9 17 19
Administrator / 10
Advanced / 14 21 24
Alert / 23 24
Alerts / 7 9 22 23
Alphabetical Index / 27
Assignee / 23
Auto-learn / 23 24

B

Basic / 11
Block / 7

C

Cast / 19 20
Change / 13 15 16 17 18 24

Co-sqlmonexe / 6 8 11 17 20 23
Column / 19 20 22
Columns / 19 22
Commit / 21
Components / 6
Components, SQL Table Monitor System Software / 6
Configuration / 6 11 16
Configuration, SQL Software / 11
Constraints / 8 19
Constraints, SQL Table Monitor / 8
Correlation / 23
Counter / 23
Counters / 23
Creating / 22
Cycle / 17 19 22 24

D

Data / 17 19
Database / 5 10 22
Debug / 20
Debug, Error Handling And / 20
Delimiter / 22
Detailed / 25
Diagram / 7
Disk / 10
Distribution / 9

E

Error / 20 22
Error Handling And Debug / 20
Existing / 10

F

Facility / 17 20
Failure / 23
Field / 22
File / 15
Firewall / 10

H

Handling / 20
Handling, Error And Debug / 20

Help / 25
How To Use This Manual / 8

I

Include / 22
Index / 18 19 20 27
Index, Alphabetical / 27
Information… / 25
Installation / 9 10
Installation, Software / 9
Installation, Windows Procedure / 10
Interval / 23 24
Introduction / 5 5
Ixcol / 20

K

Keyword / 17 19

L

Labels / 22
Logtime / 19

M

Main / 7 8
Manager / 10 11
Manual / 8 10
Manual, How To Use This / 8
Message / 14 17 19 20
Messages / 5 6 8 9 11 19 23
Mode / 18
Monitoring / 13
Monitors / 15
Ms-sql / 7 20
Msgno / 19

O

Odbc / 6 7 8 10 11 17 19 20 22
Operation / 6 13
Operation, Software / 13
Oracle / 7
Overview / 6

P

Parameters / 21
Phrase / 22
Pivot / 22
Poll / 22 23 24
Prefix / 17 19
Procedure / 10
Procedure, Windows Installation / 10
Process / 7
Program / 6

Q

Query / 17

R

Reference / 10
Relational / 5 10
Reports / 10 11 17 19 20
Requirements / 10
Restart / 11
Results / 17 24
Router / 23

S

SQL Software Configuration / 11
SQL Table Monitor Constraints / 8
SQL Table Monitor System Software Components / 6
Schedule / 6
Selecting / 18
Server / 5 7 8 9 10 11 22 25
Service / 10 11
Services / 10 11
Settings / 21
Severity / 17 20 22
Software / 6 9 11 13
Software, SQL Configuration / 11
Software, SQL Table Monitor System Components / 6
Software Installation / 9
Software Operation / 13
Source / 17 19
Space / 10

Sqlmon / 6 8 9 11
Sqlmonexe / 7 24
Start / 10 11
Step / 11
Summary / 23
Syslog / 5 6 8 13 23
System / 6 7 11
System, SQL Table Monitor Software Components / 6

T

Table, SQL Monitor Constraints / 8
Table, SQL Monitor System Software Components / 6
Tables / 5
Tail / 13 15 18 20 24
Task / 11
Threads / 7 9 22 23
Ticket / 9 23
Tickets / 22
Time / 22
Title / 17 19
Tools / 10 11 17 19
Triggers / 7
Tstamp / 19
Types / 15

U

Update / 13 15 16 17 18 24
User / 8 10

V

Verify / 11
Virus / 10
Visit / 25

W

Wait / 22 24
Windows / 6 9 10 11 14 17 19
Windows Installation Procedure / 10
Winzip / 6 9